►**B**

VERORDENING (EU) 2019/796 VAN DE RAAD

van 17 mei 2019

betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

(PB L 129I van 17.5.2019, blz. 1)

Gewijzigd bij:

		Publicatieblad		
		nr.	blz.	datum
►**M1**	Uitvoeringsverordening (EU) 2020/1125 van de Raad van 30 juli 2020	L 246	4	30.7.2020
►**M2**	Uitvoeringsverordening (EU) 2020/1536 van de Raad van 22 oktober 2020	L 351 I	1	22.10.2020
►**M3**	Uitvoeringsverordening (EU) 2020/1744 van de Raad van 20 november 2020	L 393	1	23.11.2020
►**M4**	Uitvoeringsverordening (EU) 2022/595 van de Commissie van 11 april 2022	L 114	60	12.4.2022

Gerectificeerd bij:

►**C1** Rectificatie PB L 230 van 17.7.2020, blz. 37 (2019/796)

▼B

VERORDENING (EU) 2019/796 VAN DE RAAD

van 17 mei 2019

betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

Artikel 1

1. Deze verordening is van toepassing op cyberaanvallen met aanzienlijke gevolgen, met inbegrip van pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen, die een externe bedreiging vormen voor de Unie of haar lidstaten.

2. Cyberaanvallen die een externe bedreiging vormen, omvatten onder meer die welke:

a) afkomstig zijn, of worden uitgevoerd, van buiten de Unie;

b) gebruik maken van infrastructuur buiten de Unie;

c) worden uitgevoerd door natuurlijke of rechtspersonen, entiteiten of lichamen die buiten de Unie zijn gevestigd of actief zijn; of

d) worden uitgevoerd met de steun, op aanwijzing of onder zeggenschap van natuurlijke personen of rechtspersonen, entiteiten of lichamen die buiten de Unie actief zijn.

3. Daartoe zijn cyberaanvallen acties die een van de volgende activiteiten omvatten:

a) zich toegang verschaffen tot informatiesystemen;

b) verstoren van informatiesystemen;

c) verstoren van gegevens; of

d) onderscheppen van gegevens;

indien die acties niet door de eigenaar of een andere rechthebbende van het systeem of gegevens of een deel daarvan zijn toegelaten, of niet zijn toegestaan krachtens het recht van de Unie of de betrokken lidstaat.

4. Cyberaanvallen die een bedreiging vormen voor de lidstaten omvatten die welke gevolgen hebben voor informatiesystemen in verband met onder meer:

a) kritieke infrastructuur, waaronder kabels onder zee en objecten die in de ruimte zijn gelanceerd, die van essentieel belang is voor het in stand houden van vitale functies van de maatschappij, of de gezondheid, veiligheid, beveiliging en het economische of sociale welzijn van mensen;

b) diensten die nodig zijn voor het in stand houden van essentiële sociale en/of economische activiteiten, met name in de sectoren energie (elektriciteit, olie en gas); vervoer (via de lucht, via het spoor, over water en over de weg); bankwezen; financiëlemarktinfrastructuren; gezondheidszorg (gezondheidszorgverleners, ziekenhuizen en privéklinieken); levering en distributie van drinkwater; digitale infrastructuur; en elke andere sector die voor de betrokken lidstaat van essentieel belang is;

▼B

c) kritieke functies van de staat, met name op het gebied van defensie, van het bestuur en het functioneren van instellingen, onder meer voor openbare verkiezingen of de kiesprocedure, van het functioneren van de economische en civiele infrastructuur, van de interne veiligheid, en de externe betrekkingen, onder meer via diplomatieke missies;

d) de opslag of de verwerking van gerubriceerde informatie; of

e) noodresponsteams van de overheid.

5. Cyberaanvallen die een bedreiging vormen voor de Unie omvatten die welke worden uitgevoerd tegen haar instellingen, organen en instanties, haar delegaties in derde landen of in internationale organisaties, haar operaties en missies in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) en haar speciale vertegenwoordigers.

6. Indien nodig ter verwezenlijking van de doelstellingen van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) die in de desbetreffende bepalingen van artikel 21 van het Verdrag betreffende de Europese Unie zijn vermeld, kunnen tevens beperkende maatregelen krachtens deze verordening worden toegepast in reactie op tegen derde staten of internationale organisaties gerichte cyberaanvallen met aanzienlijke gevolgen.

7. Voor de toepassing van deze verordening wordt verstaan onder:

a) „informatiesystemen”: apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op grond van een programma automatisch digitale gegevens verwerken, alsmede de digitale gegevens die met dat apparaat of die groep van apparaten worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan;

b) „verstoren van een informatiesysteem”: ernstige obstructie of onderbreking van de werking van een informatiesysteem door het invoeren, doorgeven, beschadigen, wissen, aantasten, wijzigen of onderdrukken van digitale gegevens, of door deze gegevens ontoegankelijk te maken;

c) „verstoren van gegevens”: het wissen, beschadigen, aantasten, wijzigen of onderdrukken van digitale gegevens in een informatiesysteem, of het ontoegankelijk maken van deze gegevens; hieronder valt ook diefstal van gegevens, tegoeden, economische middelen of intellectuele eigendom;

d) „onderscheppen van gegevens”: onderschepping, met technische middelen, van niet-openbare transmissies van digitale gegevens naar, vanuit of binnen een informatiesysteem, met inbegrip van elektromagnetische emissies uit een informatiesysteem dat deze gegevens bevat.

8. Voor de toepassing van deze verordening wordt bovendien verstaan onder:

a) „vordering”: een vóór of na de datum van inwerkingtreding van deze verordening ingediende vordering, ook wanneer deze de vorm van een rechtsvordering heeft, die voortvloeit uit of verband houdt met een contract of transactie, en met name:

   i) een vordering tot nakoming van een verplichting die voortvloeit uit of verband houdt met een contract of transactie;

   ii) een vordering tot verlenging of uitbetaling van een obligatie, financiële garantie of contragarantie, ongeacht de vorm;

   iii) een vordering tot schadeloosstelling in verband met een contract of een transactie;

   iv) een tegenvordering;

▼B

v) een vordering, ook via een *exequatur*, waarmee wordt beoogd erkenning of uitvoering van een rechterlijke of arbitrale uitspraak of van een gelijkwaardige beslissing te verkrijgen, ongeacht de plaats van uitspraak;

b) „contract of transactie”: een verrichting, ongeacht haar vorm en het recht dat erop van toepassing is, die een of meer contracten of soortgelijke verplichtingen tussen al dan niet dezelfde partijen omvat; in dit verband worden onder „contract” tevens begrepen alle - ook de uit juridisch oogpunt op zichzelf staande - obligaties, garanties of contragaranties, met name financiële garanties of contragaranties en kredieten, alsmede alle uit een dergelijke transactie voortkomende of daarmee verband houdende bepalingen;

c) „bevoegde autoriteiten”: de bevoegde autoriteiten van de lidstaten als aangegeven op de websites die zijn opgesomd in bijlage II;

d) „economische middelen”: activa van enigerlei aard, materieel of immaterieel, roerend of onroerend, die geen tegoeden zijn, maar kunnen worden gebruikt om tegoeden, goederen of diensten te verkrijgen;

e) „bevriezing van economische middelen”: het voorkomen van het gebruik van economische middelen om op enigerlei wijze tegoeden, goederen of diensten te verkrijgen, inclusief, maar niet daartoe beperkt, door deze te verkopen, te verhuren of te hypothekeren;

f) „bevriezing van tegoeden”: het voorkomen van het op enigerlei wijze muteren, overmaken, corrigeren en gebruiken van, toegang verschaffen tot of omgaan met tegoeden met als gevolg wijzigingen van hun omvang, bedrag, locatie, eigenaar, bezit, onderscheidende kenmerken of bestemming of elke andere wijziging waardoor het gebruik van bedoelde tegoeden, inclusief het beheer van een beleggingsportefeuille, mogelijk zou worden gemaakt;

g) „tegoeden”: financiële activa en voordelen van enigerlei aard, met inbegrip van, maar niet beperkt tot:

i) contanten, cheques, geldvorderingen, wissels, postwissels en andere betaalmiddelen;

ii) deposito's bij financiële instellingen of andere entiteiten, saldi op rekeningen, schulden en schuldbewijzen;

iii) in het openbaar en onderhands verhandelde waardepapieren en schuldbewijzen, inclusief aandelen, certificaten van waardepapieren, obligaties, promesses, warrants, schuldbekentenissen en derivatencontracten;

iv) rente, dividenden of andere inkomsten uit of waarde voortkomende uit of gegenereerd door activa;

v) krediet, recht op compensatie, garanties, uitvoeringsgaranties of andere financiële verplichtingen;

vi) kredietbrieven, cognossementen en koopbrieven; en

vii) bewijsstukken van belangen in fondsen of financiële middelen;

▼B

h) „grondgebied van de Unie”: het grondgebied van alle lidstaten waarop het Verdrag van toepassing is, onder de in het Verdrag bepaalde voorwaarden, met inbegrip van hun luchtruim.

Artikel 2

De factoren om te bepalen of een cyberaanval aanzienlijke gevolgen heeft als bedoeld in artikel 1, lid 1, punt a), kunnen onder meer de volgende zijn:

a) de omvang, schaal, impact of ernst van verstoring, ook wat betreft economische en maatschappelijke activiteiten, essentiële diensten, essentiële staatsfuncties, openbare orde of openbare veiligheid;

b) het aantal getroffen natuurlijke personen of rechtspersonen, entiteiten of lichamen;

c) het aantal betrokken lidstaten;

d) de omvang van de economische schade die bijvoorbeeld wordt veroorzaakt door diefstal op grote schaal van tegoeden, economische middelen of intellectuele eigendom;

e) het economische voordeel dat de dader voor zichzelf of anderen verkrijgt;

f) de hoeveelheid gestolen gegevens of de aard ervan, of de omvang van de gegevensinbreuken; of

g) de aard van de commercieel gevoelige gegevens waartoe toegang is verkregen.

Artikel 3

1. Alle tegoeden en economische middelen die toebehoren aan of eigendom zijn, in het bezit zijn of onder zeggenschap staan van een in bijlage I opgenomen natuurlijke persoon of rechtspersoon, entiteit of lichaam, worden bevroren.

2. Aan of ten behoeve van in bijlage I opgenomen natuurlijke personen of rechtspersonen, entiteiten of lichamen worden geen tegoeden of economische middelen direct of indirect ter beschikking gesteld.

3. In bijlage I worden opgenomen de door de Raad overeenkomstig artikel 5, lid 1, van Besluit (GBVB) 2019/797 aangewezen:

a) natuurlijke personen of rechtspersonen, entiteiten of lichamen die verantwoordelijk zijn voor cyberaanvallen of pogingen tot cyberaanvallen;

b) natuurlijke personen of rechtspersonen, entiteiten of lichamen die financiële, technische of materiële steun verlenen aan, of op enige andere wijze betrokken zijn bij cyberaanvallen of pogingen tot cyberaanvallen, met inbegrip van het plannen, voorbereiden, deelnemen aan, aansturen van, assisteren bij of aanmoedigen van dergelijke aanvallen, of het faciliteren daarvan door handelen of nalaten;

c) natuurlijke personen of rechtspersonen, entiteiten of lichamen die geassocieerd zijn met de onder de punten a) en b) vallende natuurlijke personen of rechtspersonen, entiteiten of lichamen.

▼B

Artikel 4

1. In afwijking van artikel 3 kunnen de bevoegde autoriteiten van de lidstaten, op door hen passend geachte voorwaarden, toestemming verlenen voor de vrijgave van bepaalde bevroren tegoeden of economische middelen of de beschikbaarstelling van bepaalde tegoeden of economische middelen, nadat zij hebben vastgesteld dat de betrokken tegoeden of economische middelen:

▼C1

a) noodzakelijk zijn voor het dekken van uitgaven voor de basisbehoeften van de in de bijlage I opgenomen natuurlijke personen of rechtspersonen, entiteiten of lichamen, en van de gezinsleden die van dergelijke natuurlijke personen afhankelijk zijn, zoals betalingen voor levensmiddelen, huur of hypotheeklasten, geneesmiddelen en medische behandelingen, belastingen, verzekeringspremies en nutsvoorzieningen;

▼B

b) uitsluitend bestemd zijn voor de betaling van redelijke honoraria of de vergoeding van gemaakte kosten in verband met de verlening van juridische diensten;

c) uitsluitend bestemd zijn voor de betaling van honoraria of kosten voor alleen het aanhouden of beheren van bevroren tegoeden of economische middelen;

d) noodzakelijk zijn voor de betaling van buitengewone lasten, mits de relevante bevoegde autoriteit de bevoegde autoriteiten van de andere lidstaten en de Commissie ten minste twee weken vóór zij de toestemming verleent, in kennis stelt van de redenen waarom zij meent dat specifieke toestemming dient te worden verleend; of

e) gestort zullen worden op of betaald zullen worden van een rekening van een diplomatieke of consulaire missie of een internationale organisatie die immuniteit geniet op grond van het internationaal recht, voor zover die betalingen bestemd zijn voor de officiële doelen van de diplomatieke of consulaire missie of de internationale organisatie.

2. De betrokken lidstaat stelt de andere lidstaten en de Commissie in kennis van elke toestemming die overeenkomstig lid 1 is verleend en dit binnen twee weken nadat die toestemming is verleend.

Artikel 5

1. In afwijking van artikel 3, lid 1, kunnen de bevoegde autoriteiten van de lidstaten toestemming verlenen voor de vrijgave van bepaalde bevroren tegoeden of economische middelen, mits aan de volgende voorwaarden is voldaan:

a) de tegoeden of economische middelen zijn het voorwerp van een arbitragebesluit dat is vastgesteld vóór de datum waarop de in artikel 3 bedoelde natuurlijke personen, rechtspersonen, entiteiten of lichamen werden opgenomen in bijlage I, of van een rechterlijk of administratief besluit dat in de Unie is uitgesproken, of van een rechterlijk besluit dat in de betrokken lidstaat uitvoerbaar is, en dat van voor of na die datum dateert;

b) de tegoeden of economische middelen worden uitsluitend benut om te voldoen aan de vorderingen die bij de beslissing zijn gewaarborgd of geldig zijn verklaard, overeenkomstig de wettelijke en bestuursrechtelijke voorschriften betreffende de rechten van de houders van die vorderingen;

c) de beslissing komt niet ten goede aan een in bijlage I opgenomen natuurlijke persoon of rechtspersoon, entiteit of lichaam; en

d) de erkenning van de beslissing is niet in strijd met de openbare orde van de betrokken lidstaat.

▼B

2. De betrokken lidstaat stelt de andere lidstaten en de Commissie in kennis van elke toestemming die overeenkomstig lid 1 is verleend en dit binnen twee weken nadat die toestemming is verleend.

Artikel 6

1. In afwijking van artikel 3, lid 1, en mits een betaling verschuldigd is door een in bijlage I opgenomen natuurlijke persoon of rechtspersoon, entiteit of lichaam op grond van een contract of overeenkomst dat of die is gesloten of een verplichting die is ontstaan vóór de datum waarop de betrokken natuurlijke persoon of rechtspersoon, de betrokken entiteit of het betrokken lichaam in bijlage I werd opgenomen, kunnen de bevoegde autoriteiten van de lidstaten, onder door hen passend geachte voorwaarden, toestemming verlenen voor de vrijgave van bepaalde bevroren tegoeden of economische middelen, indien de betrokken bevoegde autoriteit heeft vastgesteld dat:

a) de tegoeden of economische middelen zullen worden gebruikt voor een betaling door een in bijlage I opgenomen natuurlijke persoon of rechtspersoon, entiteit of lichaam; en

b) de betaling niet in strijd is met artikel 3, lid 2.

2. De betrokken lidstaat stelt de andere lidstaten en de Commissie in kennis van elke toestemming die overeenkomstig lid 1 is verleend en dit binnen twee weken nadat die toestemming is verleend.

Artikel 7

1. Artikel 3, lid 2, vormt geen beletsel voor de creditering van bevroren rekeningen door financiële instellingen of kredietinstellingen die tegoeden ontvangen die door derden naar de rekening van een in de lijst opgenomen natuurlijke persoon of rechtspersoon, entiteit of lichaam zijn overgemaakt, mits de bijgeboekte bedragen eveneens worden bevroren. De financiële instelling of kredietinstelling brengt de relevante bevoegde autoriteit onverwijld op de hoogte van dergelijke verrichtingen.

2. Artikel 3, lid 2, is niet van toepassing op het overmaken op bevroren rekeningen van:

a) rente of andere inkomsten op die rekeningen;

b) betalingen op grond van contracten, overeenkomsten of verplichtingen die zijn gesloten of ontstaan vóór de datum waarop de in artikel 3, lid 1, bedoelde natuurlijke personen of rechtspersonen, entiteiten of lichamen zijn opgenomen in bijlage I; of

c) betalingen die verschuldigd zijn uit hoofde van rechterlijke, administratieve of arbitragebesluiten die in een lidstaat zijn uitgesproken of in de betrokken lidstaat uitvoerbaar zijn,

mits deze rente, andere inkomsten en betalingen onderworpen blijven aan de in artikel 3, lid 1, bedoelde maatregelen.

Artikel 8

1. Onverminderd de geldende voorschriften inzake rapportage, vertrouwelijkheid en beroepsgeheim zijn natuurlijke personen en rechtspersonen, entiteiten en lichamen verplicht:

▼B

a) alle informatie die de naleving van deze verordening vergemakkelijkt, zoals informatie in verband met rekeningen en bedragen die overeenkomstig artikel 3, lid 1, zijn bevroren, onverwijld te verstrekken aan de bevoegde autoriteit van de lidstaat waar zij hun woonplaats hebben of gevestigd zijn, en deze informatie, direct of via de lidstaat, aan de Commissie te doen toekomen; en

b) samen te werken met de bevoegde autoriteit bij de verificatie van de in punt a) bedoelde informatie.

2. Alle rechtstreeks door de Commissie ontvangen aanvullende informatie wordt ter beschikking gesteld van de lidstaten.

3. Overeenkomstig dit artikel verstrekte en ontvangen informatie wordt uitsluitend gebruikt voor de doeleinden waarvoor de informatie is verstrekt of ontvangen.

Artikel 9

Het is verboden om bewust en opzettelijk deel te nemen aan activiteiten die tot doel of gevolg hebben dat de in artikel 3 bedoelde maatregelen worden omzeild.

Artikel 10

1. De bevriezing van tegoeden en economische middelen of de weigering om tegoeden of economische middelen beschikbaar te stellen, die plaatsvindt in het vertrouwen dat die maatregel in overeenstemming is met deze verordening, geeft geen aanleiding tot enigerlei aansprakelijkheid van de natuurlijke persoon of rechtspersoon of de entiteit of het lichaam die of dat die maatregel uitvoert, of van directeuren of werknemers daarvan, tenzij het bewijs wordt geleverd dat de tegoeden en economische middelen als gevolg van nalatigheid zijn bevroren of ingehouden.

2. Handelingen van natuurlijke personen of rechtspersonen, entiteiten of lichamen geven geen aanleiding tot enigerlei aansprakelijkheid van de betrokkenen, indien zij niet wisten en geen gegronde reden hadden om te vermoeden dat hun handelingen een inbreuk zouden vormen op de bij deze verordening ingestelde maatregelen.

Artikel 11

1. Vorderingen in verband met contracten of andere transacties aan de uitvoering waarvan, direct of indirect, geheel of gedeeltelijk, afbreuk is gedaan door de maatregelen die uit hoofde van onderhavige verordening zijn ingesteld, met inbegrip van vorderingen tot schadeloosstelling of soortgelijke vorderingen, zoals een vordering tot schuldvergelijking of een garantievordering, met name een vordering tot verlenging of uitbetaling van een obligatie, garantie of contragarantie, met name een financiële garantie of contragarantie, ongeacht de vorm hiervan, worden niet toegewezen indien deze vorderingen worden ingesteld door:

a) in bijlage I opgenomen natuurlijke personen of rechtspersonen, entiteiten of lichamen;

b) een natuurlijke persoon of rechtspersoon, entiteit of lichaam, handelend voor rekening of ten behoeve van een van de in punt a) bedoelde natuurlijke of rechtspersonen, entiteiten of lichamen.

2. In de procedure waartoe een vordering aanleiding geeft, wordt het bewijs dat de vordering niet op grond van lid 1 hoort te worden afgewezen, door de eisende natuurlijke persoon of rechtspersoon, de eisende entiteit of het eisende lichaam geleverd.

3. Dit artikel geldt onverminderd het recht van de in lid 1 bedoelde natuurlijke personen of rechtspersonen, entiteiten en lichamen op toetsing door de rechter van de rechtmatigheid van de niet-nakoming van contractuele verplichtingen in overeenstemming met deze verordening.

▼B

Artikel 12

1. De Commissie en de lidstaten stellen elkaar in kennis van de maatregelen die uit hoofde van deze verordening worden genomen, en verstrekken elkaar alle relevante informatie waarover zij beschikken in verband met deze verordening, in het bijzonder informatie met betrekking tot:

a) de uit hoofde van artikel 3 bevroren tegoeden en de vergunningen die krachtens de artikelen 4, 5 en 6 zijn verleend;

b) problemen in verband met schendingen en handhaving, en uitspraken van nationale rechtbanken.

2. De lidstaten stellen elkaar en de Commissie onverwijld in kennis van alle andere relevante informatie waarover zij beschikken, en die van invloed kan zijn op de doeltreffende tenuitvoerlegging van deze verordening.

Artikel 13

1. Wanneer de Raad besluit een natuurlijke persoon of rechtspersoon, entiteit of lichaam te onderwerpen aan de in artikel 3 bedoelde maatregelen, wijzigt hij bijlage I dienovereenkomstig.

2. De Raad stelt de betrokken natuurlijke persoon of rechtspersoon, de betrokken entiteit of het betrokken lichaam in kennis van het in lid 1 bedoelde besluit en van de redenen voor plaatsing op de lijst, hetzij rechtstreeks (indien het adres bekend is), hetzij door de bekendmaking van een kennisgeving, zodat die natuurlijke persoon of rechtspersoon, die entiteit of dat lichaam daarover opmerkingen kan indienen.

3. Indien er opmerkingen worden ingediend of belangrijk nieuw bewijsmateriaal wordt overgelegd, toetst de Raad de in lid 1 bedoelde besluiten en brengt hij de betrokken natuurlijke of rechtspersoon, de betrokken entiteit of het betrokken lichaam op de hoogte van het resultaat van de toetsing.

4. De lijst in bijlage I wordt regelmatig, en ten minste om de 12 maanden, getoetst.

5. De Commissie is bevoegd om bijlage II te wijzigen op basis van door de lidstaten verstrekte informatie.

Artikel 14

1. In bijlage I worden de redenen vermeld voor het op de lijst plaatsen van betrokken natuurlijke personen of rechtspersonen, entiteiten of lichamen.

2. Bijlage I bevat de informatie, indien deze beschikbaar is, die nodig is om de betrokken natuurlijke personen of rechtspersonen, entiteiten of lichamen te identificeren. Die informatie kan, wat natuurlijke personen betreft, bestaan uit namen en aliassen, geboortedatum en geboorteplaats, nationaliteit, paspoort- en identiteitskaartnummers, geslacht, adres (indien bekend) en functie of beroep. Met betrekking tot rechtspersonen, entiteiten of lichamen kan deze informatie bestaan uit namen, plaats en datum van registratie, registratienummer en plaats van vestiging.

Artikel 15

1. De lidstaten stellen de regels vast betreffende de sancties die van toepassing zijn op inbreuken op de bepalingen van deze verordening, en zij nemen alle nodige maatregelen om ervoor te zorgen dat die regels worden toegepast. De vastgestelde sancties zijn doeltreffend, evenredig en afschrikkend.

▼B

2. De lidstaten stellen de Commissie onverwijld na de inwerkingtreding van deze verordening in kennis van de in lid 1 bedoelde regels, en stellen haar in kennis van alle latere wijzigingen.

Artikel 16

1. De Commissie verwerkt persoonsgegevens voor de uitoefening van haar taken uit hoofde van deze verordening. Deze taken omvatten het volgende:

a) het toevoegen van de inhoud van bijlage I aan de elektronische geconsolideerde lijst van personen, groepen en entiteiten waarop financiële sancties van de Unie van toepassing zijn, en aan de interactieve kaart met sancties, die beide openbaar zijn;

b) het verwerken van informatie over de gevolgen van de maatregelen van deze verordening, zoals de waarde van bevroren tegoeden, alsook informatie over door de bevoegde autoriteiten verleende toestemming.

2. Voor de toepassing van deze verordening geldt de in bijlage II vermelde dienst van de Commissie als de „verantwoordelijke voor de verwerking” voor de Commissie in de zin van artikel 3, lid 8, van Verordening (EU) 2018/1725, teneinde te verzekeren dat de betrokken natuurlijke personen hun rechten uit hoofde van die verordening kunnen uitoefenen.

Artikel 17

1. De lidstaten wijzen de in deze verordening bedoelde bevoegde autoriteiten aan en identificeren deze op de in bijlage II vermelde websites. De lidstaten stellen de Commissie in kennis van elke wijziging van het adres van de in bijlage II vermelde websites.

2. De lidstaten delen de Commissie na de inwerkingtreding van deze verordening onverwijld mee wie hun bevoegde autoriteiten zijn en hoe contact met hen kan worden opgenomen, en delen haar alle latere wijzigingen mee.

3. Waar deze verordening een meldingsplicht vaststelt, of de verplichting de Commissie te informeren of op een andere wijze met haar te communiceren, wordt daartoe gebruikgemaakt van het adres en de andere contactgegevens die zijn vermeld in bijlage II.

Artikel 18

Deze verordening is van toepassing:

a) op het grondgebied van de Unie, met inbegrip van haar luchtruim;

b) aan boord van vlieg- of vaartuigen die onder de rechtsmacht van een lidstaat vallen;

c) op alle zich op of buiten het grondgebied van de Unie bevindende natuurlijke personen die onderdaan van een lidstaat zijn;

d) op alle volgens het recht van een lidstaat erkende of opgerichte rechtspersonen, entiteiten of lichamen, binnen of buiten het grondgebied van de Unie;

e) op alle rechtspersonen, entiteiten of lichamen ten aanzien van alle geheel of gedeeltelijk binnen de Unie verrichte zakelijke transacties.

▼B

Artikel 19

Deze verordening treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

▼B

BIJLAGE I

Lijst van de in artikel 3 bedoelde natuurlijke personen en rechtspersonen, entiteiten en lichamen

▼M1

A. Natuurlijke personen

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
▼M3				
1.	GAO Qiang	Geboortedatum: 4 oktober 1983 Geboorteplaats: Provincie Shandong, China Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationaliteit: Chinees Geslacht: man	Gao Qiang is betrokken bij „Operation Cloud Hopper", een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en die aanzienlijke gevolgen voor derde landen hebben. „Operation Cloud Hopper" was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid. De actor bekend als „APT10" („Advanced Persistent Threat 10") (ook bekend als „Red Apollo", „CVNX", „Stone Panda", „MenuPass" en „Potassium") voerde „Operation Cloud Hopper" uit. Gao Qiang kan worden gelinkt aan APT10, onder meer door zijn banden met de commando- en controle-infrastructuur van APT10. Bovendien had Huaying Haitai, een entiteit die op de lijst is geplaatst voor het ondersteunen en faciliteren van „Operation Cloud Hopper", Gao Qiang in dienst. Hij heeft banden met Zhang Shilong, die ook op de lijst is geplaatst in verband met „Operation Cloud Hopper". Gao Qiang heeft derhalve banden met zowel Huaying Haitai als Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Geboortedatum: 10 september 1981 Geboorteplaats: China Adres: Hedong, Yuang Road nr. 121, Tianjin, China Nationaliteit: Chinees Geslacht: man	Zhang Shilong is betrokken bij „Operation Cloud Hopper", een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en die aanzienlijke gevolgen voor derde landen hebben. „Operation Cloud Hopper" was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid.	30.7.2020

▼M3

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
			De actor bekend als „APT10” („Advanced Persistent Threat 10”) (ook bekend als „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” en „Potassium”) voerde „Operation Cloud Hopper” uit. Zhang Shilong kan worden gelinkt aan APT10, onder meer door de malware die hij heeft ontwikkeld en getest in verband met de door APT10 uitgevoerde cyberaanvallen. Bovendien had Huaying Haitai, een entiteit die op de lijst is geplaatst voor het ondersteunen en faciliteren van „Operation Cloud Hopper”, Zhang Shilong in dienst. Hij heeft banden met Gao Qiang, die ook op de lijst is geplaatst in verband met „Operation Cloud Hopper”. Zhang Shilong heeft derhalve banden met zowel Huaying Haitai als Gao Qiang.	

▼M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Geboortedatum: 27 mei 1972 Geboorteplaats: oblast Perm, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 120017582 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Alexey Minin nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland. Als ondersteunend medewerker inzake menselijke inlichtingen van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Alexey Minin deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken, die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Geboortedatum: 31 juli 1977 Geboorteplaats: oblast Moermansk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 100135556 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Aleksei Morenets nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland. Als cyberoperator van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Aleksei Morenets deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen.	30.7.2020

▼M1

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Geboortedatum: 26 juli 1981 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 100135555 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Evgenii Serebriakov nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland. Als cyberoperator van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Evgenii Serebriakov deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Geboortedatum: 24 augustus 1972 Geboorteplaats: Oeljanovsk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 120018866 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Oleg Sotnikov nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland. Als ondersteunend medewerker inzake menselijke inlichtingen van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Oleg Sotnikov deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen.	30.7.2020

▼M1

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
▼M2				
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Geboortedatum: 15 november 1990 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Nationaliteit: Russisch Geslacht: man	Dmitry Badin nam deel aan een cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) die aanzienlijke gevolgen heeft teweeggebracht. Als militaire-inlichtingenofficier van het 85e hoofdcentrum voor speciale diensten (GTsSS) van het hoofddirectoraat van de generale staf van de krijgsmacht van de Russische Federatie (GU/GRU) maakte Dmitry Badin deel uit van een team van Russische militaire-inlichtingenofficieren dat in april en mei 2015 een cyberaanval heeft uitgevoerd tegen het Duitse federaal parlement (Deutscher Bundestag). Die cyberaanval was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Geboortedatum: 21 februari 1961 Nationaliteit: Russisch Geslacht: man	Igor Kostyukov is thans hoofd van het hoofddirectoraat van de generale staf van de krijgsmacht van de Russische Federatie (GU/GRU), waar hij voorheen de eerste adjunct van de directeur was. Een van de eenheden onder zijn bevel is het 85e hoofdcentrum voor speciale diensten (GTsSS), ook bekend als „militaire eenheid 26165” (in de branche ook bekend als „APT28”, „Fancy Bear”, „Sofacy Group”, „Pawn Storm” en „Strontium”). In die hoedanigheid is Igor Kostyukov verantwoordelijk voor de cyberaanvallen die door het GTsSS zijn uitgevoerd, waaronder ook cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten. Meer bepaald namen militaire-inlichtingenofficieren van het GTsSS deel aan de cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) in april en mei 2015 en aan de poging tot inbraak in het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OVCW) in april 2018 in Nederland. De cyberaanval tegen het Duitse federaal parlement was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020

▼M1

B. Rechtspersonen, entiteiten en lichamen

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Ook bekend als: Haitai Technology Development Co. Ltd. Locatie: Tianjin, China	Huaying Haitai heeft financiële, technische of materiële steun verleend voor „Operation Cloud Hopper”, een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, en heeft die operatie gefaciliteerd. „Operation Cloud Hopper” was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid. De actor bekend als „APT10” („Advanced Persistent Threat 10”) (ook bekend als „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” en „Potassium”) voerde „Operation Cloud Hopper” uit. Huaying Haitai kan worden gelinkt aan APT10. Bovendien was Huaying Haitai de werkgever van Gao Qiang en Zhang Shilong, die beiden op de lijst zijn geplaatst in verband met „Operation Cloud Hopper”. Huaying Haitai heeft derhalve banden met Gao Qiang en Zhang Shilong.	30.7.2020
2.	Chosun Expo	Ook bekend als: Chosen Expo; Korea Export Joint Venture Locatie: Democratische Volksrepubliek Korea	Chosun Expo heeft financiële, technische of materiële steun verleend voor een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, waaronder de cyberaanvallen bekend onder de naam „WannaCry” en de cyberaanvallen tegen de Poolse autoriteit voor financieel toezicht en Sony Pictures Entertainment, alsook de cyberdiefstal bij de centrale bank van Bangladesh en de poging tot cyberdiefstal bij de Vietnamese Tien Phong Bank, en heeft deze cyberaanvallen gefaciliteerd. „WannaCry” verstoorde informatiesystemen in de hele wereld door ze met ransomware aan te vallen en door de toegang tot gegevens te blokkeren. Dit heeft gevolgen gehad voor informatiesystemen van ondernemingen in de Unie, onder meer informatiesystemen in verband met diensten voor het in stand houden van essentiële diensten en economische activiteiten in de lidstaten.	30.7.2020

▼M1

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
			De actor bekend als „APT38” („Advanced Persistent Threat 38”) of de „Lazarus-groep” hebben „WannaCry” uitgevoerd. Chosun Expo kan worden gelinkt aan APT38/de Lazarus-groep, onder meer via de rekeningen die zijn gebruikt voor de cyberaanvallen.	
3.	Het hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU)	Adres: 22 Kirova Street, Moskou, Russische Federatie	Het hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU), dat ook bekend is onder veldpostnummer 74455, is verantwoordelijk voor cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en voor cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, waaronder de cyberaanvallen van juni 2017 bekend onder de namen „NotPetya” of „EternalPetya” en de cyberaanvallen tegen een Oekraïens elektriciteitsnet in de winter van 2015 en 2016. „NotPetya” of „EternalPetya” maakte gegevens ontoegankelijk voor een aantal bedrijven in de Unie, Europa in ruimere zin, en de hele wereld, door computers aan te vallen met ransomware en door de toegang tot gegevens te blokkeren, wat onder meer tot significante economische verliezen heeft geleid. De cyberaanval op een Oekraïens elektriciteitsnet leidde ertoe dat delen ervan tijdens de winter werden uitgeschakeld.	30.7.2020
			De actor bekend als „Sandworm” (ook bekend als „Sandworm Team”, „BlackEnergy Group”, „Voodoo Bear”, „Quedagh”, „Olympic Destroyer” en „Telebots”), die ook achter de aanval op het elektriciteitsnet in Oekraïne zat, heeft „NotPetya” of „EternalPetya” uitgevoerd. Het hoofdcentrum voor speciale technologieën van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie speelt een actieve rol bij de door Sandworm uitgevoerde cyberactiviteiten en kan aan Sandworm worden gelinkt.	

▼M1

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
▼M2				
4.	85e hoofdcentrum voor speciale diensten (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU)	Adres: Komsomol'skiy Prospekt, 20, Moskou, 119146, Russische Federatie	Het 85e hoofdcentrum voor speciale diensten (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU), ook bekend als „militaire eenheid 26165” (in de branche ook bekend als „APT28”, „Fancy Bear”, „Sofacy Group”, „Pawn Storm” en „Strontium”), is verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten. Meer bepaald namen militaire-inlichtingenofficieren van het GTsSS deel aan de cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) in april en mei 2015 en aan de poging tot inbraak in het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OVCW) in april 2018 in Nederland. De cyberaanval tegen het Duitse federaal parlement was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020

▼B

BIJLAGE II

Websites voor informatie over de bevoegde autoriteiten en adres voor kennisgevingen aan de Commissie

▼M4

BELGIË

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIJE

https://www.mfa.bg/en/EU-sanctions

TSJECHIË

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DENEMARKEN

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

DUITSLAND

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTLAND

https://vm.ee/et/rahvusvahelised-sanktsioonid

IERLAND

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRIEKENLAND

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

SPANJE

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANKRIJK

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

KROATIË

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIË

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CYPRUS

https://mfa.gov.cy/themes/

LETLAND

http://www.mfa.gov.lv/en/security/4539

LITOUWEN

http://www.urm.lt/sanctions

LUXEMBURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

HONGARIJE

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M4**

MALTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

NEDERLAND

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

OOSTENRIJK

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLEN

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGAL

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

ROEMENIË

http://www.mae.ro/node/1548

SLOVENIË

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOWAKIJE

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLAND

https://um.fi/pakotteet

ZWEDEN

https://www.regeringen.se/sanktioner

Adres voor kennisgevingen aan de Europese Commissie:

Europese Commissie

Directoraat-generaal Financiële Stabiliteit, Financiële Diensten en Kapitaalmarkttenunie (DG FISMA)

Spastraat 2

B-1049 Brussel, België

E-mail: relex-sanctions@ec.europa.eu